AO 106 (Rev. 04/10) Application for a Search Warrant

USAO No. 2018R01020

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Dropbox Inc. Account: 335guy99@gmail.com; User ID: 244407669

Case No. MJ19-5006

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):* Subject Dropbox Account as further described in the Affidavit and Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B, which is attached hereto an incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252(a)(2)	Receipt or Distribution of Child Pornography
18 U.S.C. § 2252(a)(4)(B)	Possession of Child Pornography

The application is based on these facts:
See Affidavit of Special Agent Liam Noone, AFOSI, which is attached hereto and incorporated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

LIAM NOONE, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 01/18/2019

Judge's signature

City and state: Tacoma, Washington

J. Richard Creatura, United States Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF PIERCE)

I, Liam Noone, being duly sworn on oath, depose and state:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Air Force Office of Special Investigations (AFOSI), assigned to Detachment 305, Joint Base Lewis-McChord, Washington. I have been employed as an AFOSI Special Agent since June 2018. In my capacity as a Special Agent, I am responsible for conducting investigations into the numerous federal laws enforced by AFOSI. Since June 2018, I have investigated criminal violations relating to child exploitation and child pornography, including violations pertaining to the unlawful distribution, receipt, attempted receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A(a). I am a graduate of the Federal Law Enforcement Training Center (FLETC) Criminal Investigator Training Program and AFOSI Basic Special Investigator Course. Throughout my career I have received training in conducting criminal investigations, law enforcement techniques, federal criminal statutes, the collection and preservation of physical and digital evidence, and the execution of search warrants. I have had the opportunity to observe and review multiple examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution of search warrants which involved child pornography offenses and the search and seizure of computers and other digital devices. I work with other federal, state, and local law enforcement personnel investigating, among other things, crimes involving the sexual exploitation of children.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

2. I make this Affidavit in support of an application, pursuant to 18 U.S.C. §§ 2703(a) and 2703(c)(1)(A), for a warrant to search any and all information for the Dropbox Inc. (hereinafter referred to as "Dropbox") account "335guy99@gmail.com," User ID: 244407669, (hereafter referred to as the SUBJECT ACCOUNT), to include any and all associated cloud storage accounts and their contents, including without limitation any electronic files that the subscriber has stored in the accounts. The SUBJECT ACCOUNT is controlled by Dropbox. This application seeks a warrant to search the SUBJECT ACCOUNT and seize the items listed in Attachment B, which is attached to this Affidavit and incorporated herein by reference, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography).

3. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

4. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only the facts necessary to determine there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), will be found in the SUBJECT ACCOUNT.

II. TECHNICAL BACKGROUND

5. In my training and experience, I have learned that Dropbox was founded in 2007 and is a privately held electronic file storage service headquartered in San Francisco, California. Dropbox is a file hosting service that allows users to upload and

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

synchronize files to cloud storage and then access them from a web browser or application on their computer or digital device. It is a simple online virtual storage utility that allows users to make their files accessible from almost anywhere. Dropbox allows users to keep the files private, share them with contacts, or make the files public. Dropbox also allows users to create a special folder or link on their computers or digital devices, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which computer or device is used to access it. Files placed in this folder are also accessible via the Dropbox website and mobile apps. Dropbox users can also share files or folders they create with other Dropbox users. Dropbox provides both free and fee-based file sharing and file synchronization services. Dropbox stores files in user accounts until the user deletes them. Dropbox saves deleted files for 30 days. If a Dropbox account is deleted, the files and account information will be purged after 30 days.

6. Dropbox users create Dropbox accounts, which are identified by the user's e-mail address and secured with a user password. The e-mail address is the unique identifier for a Dropbox account. Once an account is created with Dropbox, the user must enter his or her e-mail address for the account along with a valid user-created password in the login screen in order to access the account. Since Dropbox accounts are not publicized and the general login screen does not show other valid e-mail accounts, the user must know the e-mail address in the first step to access a Dropbox account. Users are also able to utilize the login with Google option and enter their Google credentials to access a Dropbox account which will be linked to the Google account.

7. Cloud storage providers like Dropbox typically retain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Dropbox's website or

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

application), and other log files that reflect usage of the account. In addition, cloud storage providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the cloud storage account, which can help establish the individual or individuals who had dominion and control over the account.

8. Dropbox conducts business throughout the United States and the world through its file-sharing services.

9. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals involved in child pornography:

10. Those who receive and attempt to receive child pornography over the Internet often maintain their collections which are in a digital or electronic format in a safe, secure and private environment, such as a computer or cloud storage service. These collections are often maintained for several years and are kept where the individual can easily access them, such as at the individual's residence or on a digital or electronic storage device.

11. Those who receive and attempt to receive child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

12. Those who receive and attempt to receive child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

13. In the case of those who receive and attempt to receive child pornography via email, the nature of email itself provides a convenient means by which these individuals can access their collections from any computer, at any location with Internet access. These individuals therefore do not need to physically carry their collections with them, but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

14. The National Center for Missing and Exploited Children (NCMEC) is a private non-profit organization operating under a Congressional mandate to act as the nation's law enforcement clearing house for information concerning online child sexual exploitation. In partial fulfillment of that mandate, NCMEC operates a CyberTip line, a resource for reporting online crimes against children. Electronic Service Providers (ESPs) report to NCMEC, via the CyberTip line, whenever they discover that a subscriber has violated the terms of service and/or their services have been used to store or transmit child pornography over the Internet.

15. Any incidents reported to the CyberTip line online or by telephone go through this three-step process: CyberTip line operators review and prioritize each lead; NCMEC's Exploited Children Division analyzes tips and conducts additional research; the information is accessible to the Federal Bureau of Investigations, Immigrations and Customs Enforcement, United States Secret Service, and the United States Postal Inspection Service. Information is also forwarded to the Internet Crimes Against Children Taskforces and pertinent international, federal, state, and local authorities and, when appropriate, to the ESP.

16. A hash value is an alphanumeric sequence that is unique to a specific digital file. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

results in a different hash value. Consequently, an unknown image can be determined to be identical to an original file if it has the same hash value as the original. The hash value is, in essence, the unique "fingerprint" of that file, and when a match of the fingerprint occurs, the file also matches.

17. ESPs typically maintain a database of hash values of files that they have determined to meet the federal definition of child pornography found in 18 USC § 2256. The ESPs typically do not maintain the actual suspect files themselves; once a file is determined to contain suspected child pornography, the file is deleted from their system. The ESPs can then use Image Detection and Filtering Process, Photo DNA, or a similar technology which compares the hash values of files embedded in or attached to transmitted files against their database containing what is essentially a catalog of hash values of files that have previously been identified as containing suspected child pornography.

18. The hash values in the transmitted file(s) are contained in the "metadata" associated with the files. This "metadata" is "data about data," e.g. information about the file that is created and used at various times along the creation, transmission, and receipt of the file. For example metadata may include information about what language it is written in, what tools were used to create it, sender information, and what sort of files are associated with it.

19. When an ESP detects a file passing through its network that has, in its metadata, the same hash value as an image or video file of suspected child pornography contained in the database through a variety of methods, the ESP reports that fact to NCMEC via the CyberTip line. By statute, an ESP has a duty to report to NCMEC any apparent child pornography it discovers "as soon as reasonably possible." The CyberTip line report transmits the intercepted file(s) to NCMEC. The ESP is not required to open or view the file(s) because the files hash value, or "fingerprint," has already been associated to a file of suspected child pornography. The ESP's decision to report a file to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

NCMEC can be based solely on the match of the unique hash value of the suspected child pornography to the identical hash value in the suspected transmission.

III. STATEMENT OF PROBABLE CAUSE

20. KIK messenger is an application available for download on mobile devices such as smartphones and tablets. The application allows individuals to establish user accounts and then exchange messages and files (such as photos and videos) over the Internet. KIK allows users to contact other users individually, as well as to post messages in public forums, chat in groups, and exchange messages and files with other KIK users.

21. Between April 21, 2017, and May 12, 2017, investigators discovered KIK messenger user "335guy99@gmail.com" was an active member of the known KIK messenger child pornography group "Boys Links Only! Send on Entry or Ban."

22. Prior to identifying this specific user, investigators had already determined that the KIK group "Boys Links Only! Send on Entry or Ban" distributed, advertised, facilitated, discussed, accessed, viewed, and/or downloaded thousands of videos and images of child pornography. Agents had then identified certain users accessing this KIK group. One of these users, "335guy99@gmail.com," accessed the KIK messenger group from IP addresses maintained by internet service provider Comcast Cable. A subpoena was sent to Comcast who identified the subscriber to these IP addresses was identified as Jonel Har GUIHAMA, 1524 203rd Street Court East, Spanaway, WA, 98387; (253) 293-8182; guihama@comcast.net; roxannehorner88@comcast.net.

23. On September 5, 2018, FBI South Sound Exploitation Task Force and multiple AFOSI members executed a federal search warrant at GUIHAMA's residence, located at 1524 203rd Street Court East, Spanaway, WA. During the search, GUIHAMA's cellphone, laptop and an external hard drive were seized and given a preliminary analysis by AFOSI SA Joel Fry, Digital Forensic Consultant. During later analysis, SA Fry found over 5,000 images that were scanned and returned with a known Project Vic hash value match for known child pornography and another approximately

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

5,000 child erotica images with known Project Vic hash values. In addition, SA Fry found approximately 7,000 suspected child pornography images and approximately 6,000 suspected child erotica images, which are still pending further analysis.

24. Agents specifically recovered an image labeled "051.jpg" that was located on the Laptop within a file named: "*C:\Lost Files\10yr old Girl in different positions\.*" CID Digital Forensics Examiner Ray Rivera examined the image and determined it had a positive MD5 hash that matched with the NCMEC hash set library in which the depicted Caucasian female had previously been identified as a minor. The picture depicted the minor exposing her naked vaginal area and anus. An adult male's fully erect penis is immediately adjacent to the minor and about to penetrate the minor's exposed anus. The file contained an Alternate Data Stream (ADS) with an identifier usually indicative of the file being downloaded from a website on the internet.

25. On September 5, 2018, GUIHAMA was advised of his constitutional rights, which he waived prior to being interviewed. During the interview, GUIHAMA admitted to possessing and distributing child pornography through the KIK messenger application by using Dropbox links. When asked what files were in the Dropbox link he shared, GUIHAMA responded "it was bad stuff." GUIHAMA stated the files included some "younger folks" that were "in their teens." When specifically asked about the age range of the minors depicted in the files, GUIHAMA responded, "it's underage I know that for sure." GUIHAMA estimated the youngest child depicted in the files was 12-13 years old and stated some of the children were nude.

26. GUIHAMA also described the method by which he used Dropbox links during his KIK chats. GUIHAMA stated that he obtained Dropbox links from other groups on KIK. GUIHAMA would then copy the link and share it in a separate group chat when someone requested it from him. GUIHAMA acknowledged that the Dropbox links contained images and videos of minors, some of which depicted nudity and sexual acts involving minors.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

27. During the interview, GUIHAMA identified at least three KIK messenger username accounts that he had used including "335guy99@gmail.com." GUIHAMA created the "335guy99@gmail.com" KIK messenger username in the summer of 2015. GUIHAMA believed that he shared his first Dropbox link using the "335guy99@gmail.com" account in approximately February of 2016. GUIHAMA did not recall using the "335guy99@gmail.com" username after February of 2017.

28. A Department of Defense Inspector General Subpoena was served on Dropbox and confirmed the User ID for the username "335guy99@gmail.com" is 244407669.

IV. PRIOR EFFORTS TO OBTAIN EVIDENCE

29. Based upon my experience and training, it is not uncommon for technically sophisticated criminals to use encryption or programs to destroy data which can be triggered remotely or by a pre-programed event or keystroke, or other sophisticated techniques to hide data. In this case the data sought is stored on a server belonging to Dropbox. If data is accessed and deleted by the user, by either deleting the emails or any associated contact lists, the content would not be retrievable. Unlike traditional computer forensics where a hard drive can be searched and deleted documents recovered, information stored in an enterprise storage system is irretrievable once it has been deleted. Further, since this information is accessible from anywhere the suspect can obtain an Internet connection to log on to his account, they can delete this information in a matter of minutes.

30. GUIHAMA did not provide access to the SUBJECT ACCOUNT, and Dropbox has indicated it will only provide the contents of said account pursuant to a valid legal process. There are no other means of obtaining the necessary evidence to prove the elements of computer/Internet-related crimes, the only effective means of collecting and preserving the required evidence in this case is through the instant search. Based on my knowledge, no prior search warrant has been obtained to search the SUBJECT ACCOUNT.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

V. PROTOCOL FOR SORTING SEIZABLE ELECTRONCALLY STORED INFORMATION

31. In order to ensure agents are limited in their search only to the contents of the SUBJECT ACCOUNT as described in Attachment B; in order to protect the privacy interests of other third parties who have accounts at Dropbox; and in order to minimize disruptions to normal business operations of Dropbox; this application seeks authorization to permit agents and employees of Dropbox to assist in the execution of the warrant, pursuant to 18 U.S.C. § 2703(g), as follows:

a. The search warrant will be presented to Dropbox, with direction that it identify and isolate the SUBJECT ACCOUNT and associated records described in Section I of Attachment B.

b. Dropbox will also be directed to create an exact duplicate in electronic form of the SUBJECT ACCOUNT and associated records specified in Section I of Attachment B, including an exact duplicate of the content of all email messages stored in the SUBJECT ACCOUNT.

c. Dropbox shall then provide an exact digital copy of the contents of the SUBJECT ACCOUNTS, as well as all other records associated with the account, to me, or to any other agent of AFOSI. Once the digital copy has been received from Dropbox, that copy will, in turn, be forensically imaged and only that image will be reviewed and analyzed to identify communications and other data subject to seizure pursuant to Section II of Attachment B. The original digital copy will be sealed and maintained to establish authenticity, if necessary.

d. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

Certain file formats, moreover, do not lend themselves to keyword searches, as keywords search text, and many common electronic mail, database, and spreadsheet applications (which may be attached to email) do not store data as searchable text. The data is saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months.

e. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to seize all emails, chat logs, documents, shared links, and IP addresses which identify any users that have accessed the SUBJECT ACCOUNT and any emails sent or received in temporal proximity to incriminating emails which provide context to the incriminating communications.

f. All forensic analysis of the image data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

VI. CONCLUSION

32. Based upon the evidence gathered in this investigation as set out above, including but not limited to my review of data and records, information received from other law enforcement agents, and my training and experience, there is probable cause to believe evidence, fruits and/or instrumentalities of the crimes of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) exists and will be found in the electronically stored information or communications contained and associated with the SUBJECT ACCOUNT and any attachments, stored instant messages, stored voice messages, documents, videos, and photographs associated therewith, as well as in subscriber and log records associated with the account. Accordingly, by this Affidavit and warrant I seek authority pursuant to

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

18 U.S.C. §§ 2703(a) and 2703(c)(1)(A) for the government to search all of the items specified in Attachment A and Section I of Attachment B (attached hereto and incorporated by reference herein) to the warrant, and specifically to seize all of the data, documents and records which are identified in Section II of Attachment B.

Dated this 18th day of January, 2019.

LIAM NOONE, Affiant
Special Agent
Office of Special Investigations
United States Air Force

SUBSCRIBED and SWORN to before me this 18th day of January, 2019.

J. RICHARD CREATURA
United States Magistrate Judge

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

ATTACHMENT A

Place to be Searched

All information associated with the Dropbox account "335guy99@gmail.com," User ID: 244407669, stored at premises owned, maintained, controlled, or operated by Dropbox, a company headquartered at 185 Berry Street, Suite 400, San Francisco, California.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

ATTACHMENT B

Section I - Items to be to be Provided by Dropbox Inc. for Search

1. All electronically stored information and communications contained in the Dropbox account 335guy99@gmail.com, User ID: 244407669, associated with the period between February 1, 2016, and September 5, 2018, including associated email addresses; alternate email addresses; associated cloud storage; account registration information, user contact information, linked web addresses and posted images, content and logs; including a copy of these accounts.

2. All subscriber records associated with the period between February 1, 2016, and September 5, 2018 and the SUBJECT ACCOUNT, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

3. Log records between February 1, 2016, and September 5, 2018, including IP address captures, associated with the specified accounts;

4. Any address lists or buddy/contact lists associated with the specified account(s); and

5. Any records of communications between Dropbox Inc., between February 1, 2016, and September 5, 2018, and any other person about issues relating to the accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscribers and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Section II - Items to be Seized

All electronically stored information and communications contained in the Dropbox account 335guy99@gmail.com, User ID: 244407669, between February 1,

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800

2016, and September 5, 2018, including associated email addresses; alternate email addresses; associated cloud storage accounts to include contents of electronic files:

a. All messages, documents, and profile information, attachments, or other data between February 1, 2016, and September 5, 2018, that serves to identify any persons who use or access the accounts specified, or who exercise in any way any dominion or control over the specified accounts;

b. Any address lists or buddy/contact lists associated with the specified accounts between February 1, 2016, and September 5, 2018;

c. All images of child pornography and any messages, documents and profile information, attachments, or other data related to child pornography or the possession, receipt, or distribution of child pornography;

d. All subscriber records associated with the SUBJECT ACCOUNT between February 1, 2016, and September 5, 2018, including name, address, records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, (including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number(s);

e. Any and all other log records, including IP address captures, associated with the SUBJECT ACCOUNT between February 1, 2016, and September 5, 2018; and

f. Any records of communications between Dropbox Inc. and any person between February 1, 2016, and September 5, 2018, about issues relating to the specified accounts, such as technical problems, billing inquiries, or complaints from other users about the specified accounts. This is to include records of contacts between the subscriber and the provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

Notwithstanding the criminal offenses defined under 18 U.S.C. § 2252 and 2252A or any similar criminal offense, Dropbox Inc. shall disclose information responsive to this warrant by mailing it to Office of Special Investigations, Attn: Special Agent Liam Noone, Detachment 305, 160 McCarthy Blvd, Joint Base Lewis-McChord, Washington 98438 or via e-mail to liam.noone.2@us.af.mil.

UNITED STATES ATTORNEY
1201 PACIFIC AVENUE, SUITE 700
TACOMA, WASHINGTON 98402
(253) 428-3800